eSecurity Advisory
Microsoft Internet Explorer Zero-Day Exploit

A vulnerability has been identified in **Microsoft Internet Explorer** that could allow an attacker to run programs on a Windows system with all currently available patches applied.

This vulnerability can be exploited if a user visits a malicious web page *which is specifically crafted to exploit this vulnerability*. There is publicly available exploit code for this vulnerability.

Recommendations are provided to minimize risk.
There is currently no patch available for this issue.

What can you do?

- Disable or enable prompting for Active Scripting in Internet Explorer per the advisory from Microsoft if the adverse effects of limited web functionality do not adversely impact your business requirements.
- Do not visit unknown or un-trusted websites or follow links provided by unknown or un-trusted sources.
- Only use Internet Explorer as a non-privileged user (one without administrative privilege) to diminish the effects of a successful attack.
- Consider temporary use of an alternate browser until such time as a patch is available.

These recommendations in no way provide complete protection from this type of malicious attack, but only limit the overall exposure to the vulnerability that remains on the host until patched.

Listed below is more information that may helpful to users to protect their work and home computers.

SUBJECT:
New Microsoft Internet Explorer Zero-Day Exploit

SYSTEMS AFFECTED:

- Internet Explorer 5.0.1 (SP 1-4)
- Internet Explorer Version 6 (SP 1-2)

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Microsoft Internet Explorer that could allow arbitrary code execution on a fully patched Windows system with the privileges of the user running Internet Explorer. This vulnerability can be exploited if a user visits a malicious web page which is specifically crafted to exploit this vulnerability.

This issue is due to a flaw in the 'createTextRange()' JavaScript/DHTML method. This method can cause Internet Explorer to dereference an invalid table pointer, thereby transferring program execution flow to an arbitrary place in memory. This flaw can be exploited by a remote attacker to crash the affected browser or to run arbitrary code in the context of the user.

We have tested the proof of concept code and confirmed remote code execution. However, when tested with an alternate browser, Mozilla Firefox, the proof of concept code did not execute.

Microsoft has not released a patch to address this issue at this time.

REFERENCES:

Microsoft
http://www.microsoft.com/technet/security/advisory/917077.mspx

Security Focus
http://www.securityfocus.com/bid/17196

AUSCert
http://www.auscert.org.au/6155

SANS
http://isc.sans.org/diary.php?storyid=1209

Secunia
http://secunia.com/advisories/18680/